SOLUTION BRIEF

FortiWeb and ImmuniWeb AI

Web Application Security Testing and Agile Virtual Patching

Virtual patching is a great method to protect web applications until they can be permanently fixed by developers. ImmuniWeb and Fortinet now offer an integrated solution that audits web applications and web services (REST/SOAP) for vulnerabilities with High-Tech Bridge ImmuniWeb AI and then reliably protects them with FortiWeb virtual patching. Once a vulnerability is discovered, it is protected by FortiWeb instead of issuing disruptive emergency patches or worse, waiting weeks or months for developers to deploy a new release while the application sits unprotected.

FortiWeb virtual patching uses a combination of sophisticated tools such as URLs, parameters, signatures, and HTTP methods to create a granular rule that addresses each specific vulnerability discovered by ImmuniWeb AI. A zero false-positives SLA is provided by ImmuniWeb AI to every customer, guaranteeing safe and reliable virtual patching that will not impact web application firewall (WAF) performance or website availability.

While virtual patching will not replace the traditional application development process, it can create a secure bridge between the time a vulnerability is discovered and the time a software release is issued to address it. In cases where it may not be possible or practical to change the application code, such as with legacy, inherited and third-party applications, FortiWeb virtual patching can provide a permanent security solution for vulnerabilities.

ImmuniWeb AI uses its award-winning machine learning and AI technology for intelligent automation and acceleration of application security testing. The technology is enhanced with scalable and cost-effective manual testing when required, reliably detecting even the most intricate vulnerabilities and flaws in business logic. FortiWeb complements ImmuniWeb AI with granular application protection rules that take the imported vulnerability results and provide immediate mitigation with the same level of accuracy. This granular virtual patching is able to maintain application security until development teams are able to fully deploy permanent fixes in the application code. It can also extend the windows between security patches to minimize disruptions to the organization and its users.

Joint Solution Benefits

Using FortiWeb with High-Tech Bridge ImmuniWeb AI gives organizations :

- An enhanced solution that exceeds PCI DSS 6.5/6.6/11.3 and GDPRArt. 25/Art. 35.
- Absolute visibility across sophisticated web application vulnerabilities, weaknesses, and privacy issues.
- Prevention of data breaches and targeted attacks via corporate web applications
- Minimized risk of exposure to threats between the time a threat is discovered until it is fixed by developers.
- Less disruptions due to emergency fixes and test cycles by virtually patching vulnerabilities until they can be permanently fixed.
- Protection for legacy, inherited, and third-party applications where development fixes are not an option or are impractical.
- More stability in application security patches as developers have more time to properly fix code vs. issuing emergency patches that have not had time to be fully tested.
- More accurate FortiWeb reporting and identification of attempts to exploit vulnerabilities discovered by ImmuniWeb.
- Additional flexibility and granular management of FortiWeb WAF policies based on ImmuniWeb AI audit results.

Fabric-Ready

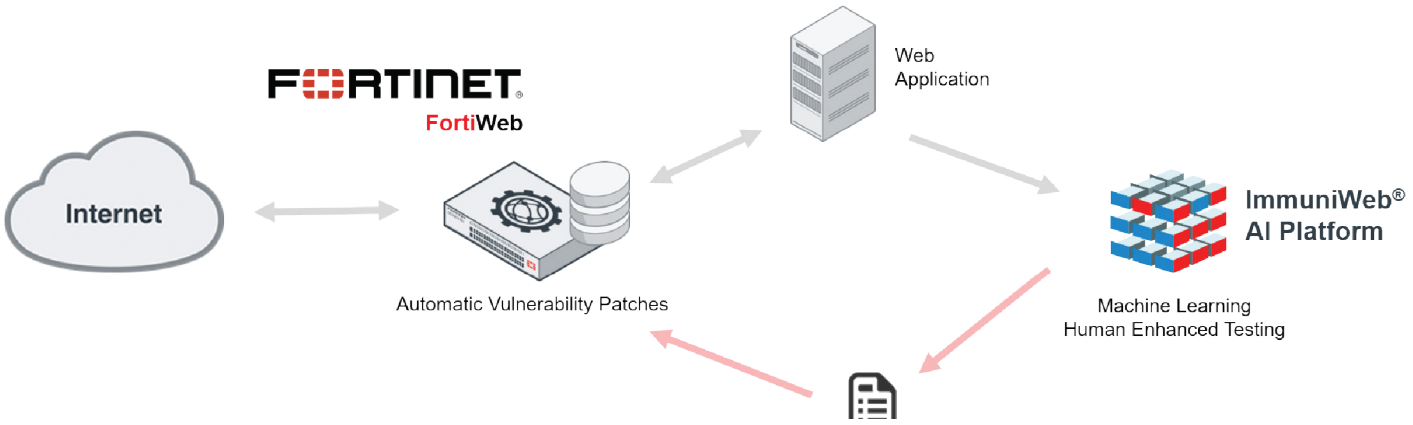

Figure 1: Once ImmuniWeb AI Audit Results are imported to FortiWeb, then FortiWeb Virtual Patching automatically creates new WAF rulesets to protect against newly discovered vulnerabilities and weaknesses.

About Fortinet

Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments—be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands.

Learn more at www.fortinet.com, the **Fortinet Blog** or **FortiGuard Labs.**

About ImmuniWeb

High-Tech Bridge is a global provider of web and mobile application security testing services. Named "Gartner Cool Vendor" and the winner in "Best Usage of Machine Learning/AI" by SC Awards Europe 2018, High-Tech Bridge pioneers the application security testing market with scalable and cost-effective application security testing products for web and mobile applications. ImmuniWeb AI Platform leverages machine learning and AI technology for intelligent automation and acceleration of application security testing. Complemented by scalable and cost-effective manual testing, it detects the most sophisticated vulnerabilities and comes with a zero false-positives SLA for every customer.

Learn more at www.htbridge.com.

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

April 25, 2019 6:39 AM

329416-0-0-EN

F:\Fortinet\PDF Files\Fortinet Fabric New Solutions Brief\sb-fortiweb-htb V1